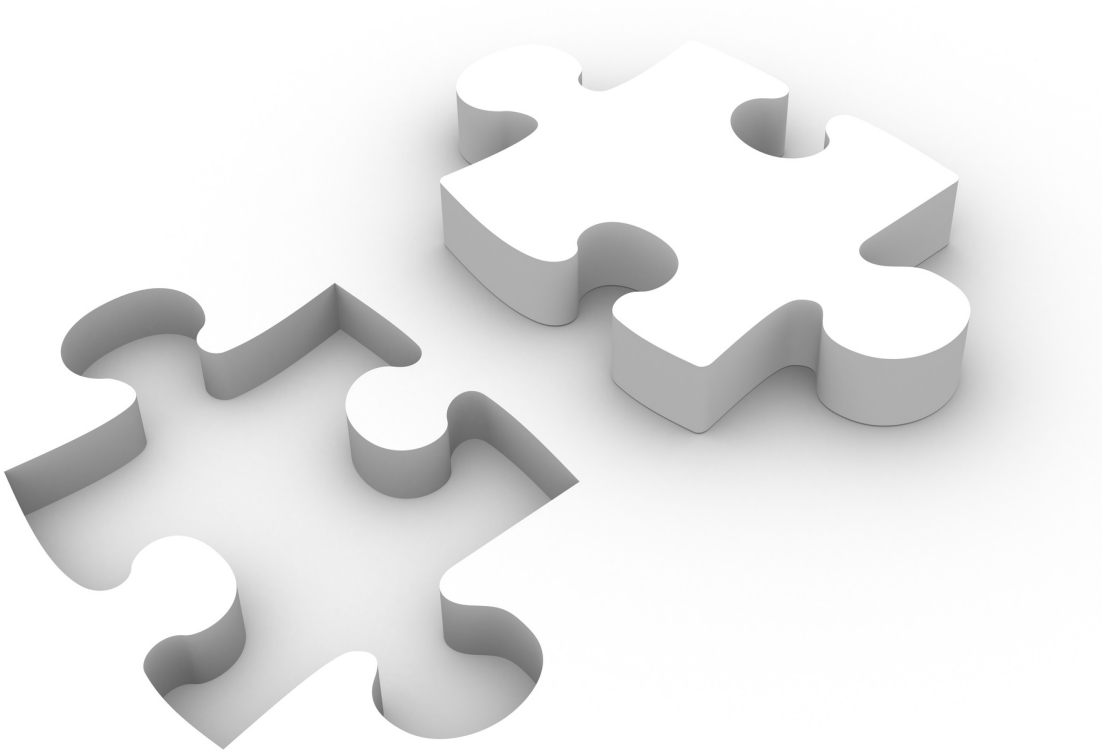
analytiq consulting gmbh

nitrobit policy extensions

Effective data loss prevention with
encrypting USB-Sticks



nitrobit
policy extensions

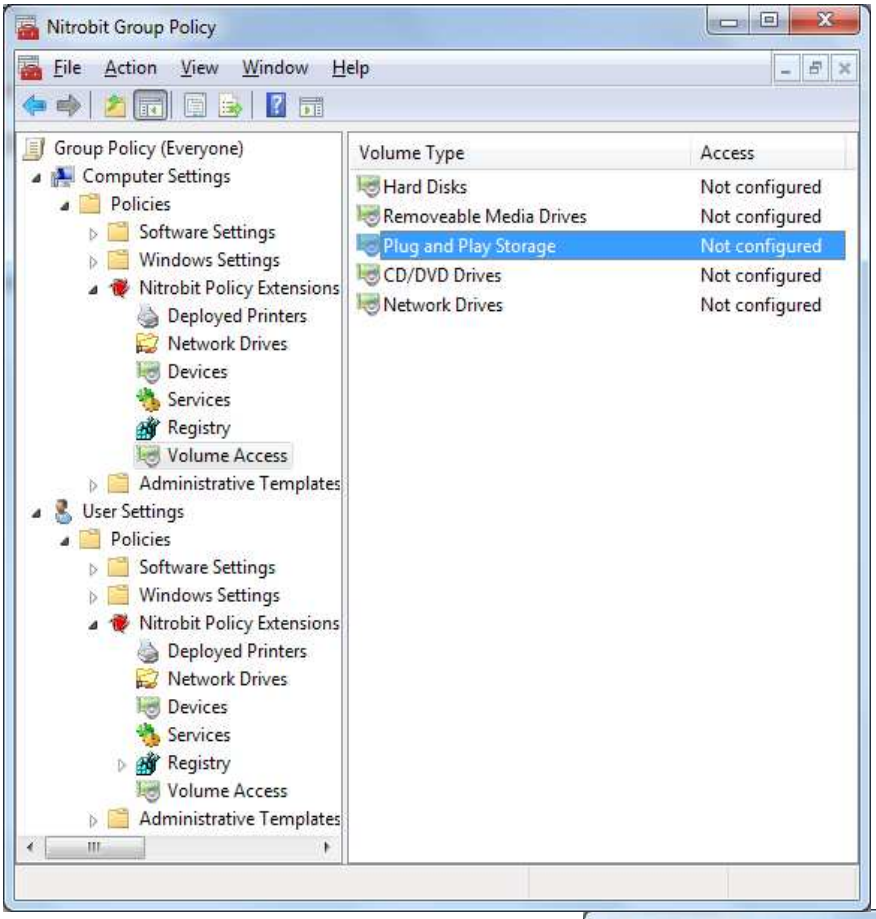
Introduction

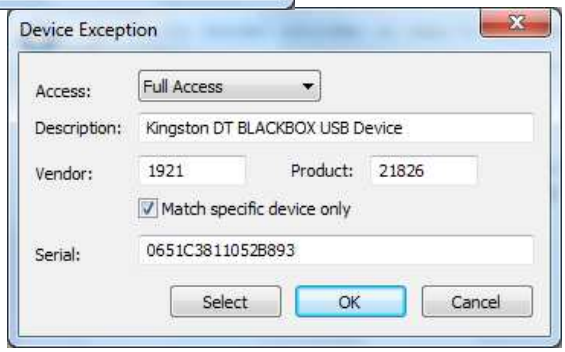
Nitrobit policy extensions provide useful extensions to Windows™ group policies. One of those extensions enforce data loss prevention policies.

The Kingston™ DataTraveler Blackbox USB flash drive provides secure portable storage by using a hardware-based 256 bit AES encryption. This document shows how to establish a secure data loss prevention solution in you corporate network easily.

Configuration

After opening the group policy object, you can find nitrobit policy extensions' volume policies under “Computer Settings” or “User Settings” → “Policies” → “Nitrobit Policy Extensions” → “Volume Policies”.





You can open the properties for the plug and play storage devices by double-clicking on the entry. On the following page, change the default access to “Read only” or “No access”.

Next, add a device exception by the “Add” button on the “Device Exceptions” page. Please select “Full access” for the access method. After that, you can browse for the Kingston™ DataTraveler Blackbox USB flash drive or you can enter product and vendor id directly.

Note: It is more secure to provide a serial number and select the option “Match specific device only”, because then the exception is only valid for these specific flash drives.

Finally, after closing the group policy editor, the changes will become active upon the next group policy refresh.

Contact

analytiq consulting gmbh
Hermann-Steinhäuser-Straße 43-47
63065 Offenbach
Germany

Tel: +49 (69) 1730 9891 0
Fax: +49 (69) 1730 9891 1
E-Mail: support@nitrobit.com
Web: www.nitrobit.com